IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application for: Avaya Technology Corp.

Art Unit: 2152

First Named Inventor: HEPWORTH, et al.

Examiner: TRUONG, LAN DAI T

Appln. No.: 10/028,874

Confirmation No.: 4659

Filing Date: October 22, 2001

For: "Real Time Control Protocol Session Matching"

* * *

APPELLANTS' BRIEF
(37 CFR § 41.37)

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Appellants hereby appeal to the Board of Appeals in response to the Notice of Panel Decision from Pre-Appeal Brief Review of August 20, 2007. The fee set forth in 37 CFR § 41.20(b) has been previously submitted in connection with the Request for Pre-Appeal Brief Request for Review. Although Appellants believe that no additional fees are due at this time, authorization to charge any necessary fees to Deposit Account No. 19-1970 is hereby given.

A single copy of this Appeal Brief is being submitted pursuant to MPEP § 1205.02.

(I) REAL PARTY IN INTEREST

All right, title, and interest in this application has been assigned by the inventors, Neil Hepworth and Alastair J. Rankine to Avaya Technology Corp. This Assignment is recorded at Reel/Frame 012448/0622.

(II) RELATED APPEALS AND INTERFERENCES

There are no related appeals, interferences or judicial proceedings known to Appellants, or the Appellants' legal representative which may be related to, directly affect, be directly affected by, or have a bearing on the Board's decision in the pending appeal.

(III) STATUS OF CLAIMS

Claims 31-56 are pending in the application. Claims 1-30 have been canceled. No claims have been withdrawn from consideration. Accordingly, Claims 31-56 are being appealed.

Claims 31-56 stand rejected under 35 U.S.C.§103(a).

The Claims at issue (*i.e.*, Claims 31-56) are set forth in the CLAIMS APPENDIX.

(IV) STATUS OF AMENDMENTS

An amendment was filed on May 29, 2007, subsequent to the Examiner's Final Office Action dated March 29, 2007. That amendment was entered by the Examiner in an Advisory Action dated June 19, 2007 ("Advisory Action").

(V) SUMMARY OF CLAIMED SUBJECT MATTER

A common architecture for VoIP is to have a session monitor, in addition to each endpoint, to effect session management. (*See* Specification page 1, lines 9-21.) To enable the monitor to obtain RTCP packets, a dual unicast architecture was developed. (*See* Specification page 2, lines 13-14.) In dual unicast, one session participant (A) transmits both RTP and RTCP packets to the other session participant (B) and RTCP packets to the monitor. (*See* Specification page 2, lines 14-15.) Dual unicast, however, exposes design

limitations in the RTCP protocol itself. (*See* Specification page 2, lines 15-16.) Although endpoint session ids are unique to a particular (first) session (such as between A and B), an endpoint in a concurrent (second) session (such as between C and D) can have the same session id or synchronization source id ("SSRC") as an endpoint (A or B) in the other (first) session. (*See* Specification page 2, lines 16-19; Fig. 1.) When duplicate endpoint session ids are concurrently in use, the monitor can have substantial difficulty determining which RTCP packets correspond to which session, potentially causing inaccurate performance analysis. (*See* Specification page 2, lines 20-22.) This is so because the RTCP packets sent to the monitor include the address of only the source endpoint and exclude the address(es) of the other endpoint(s) to the session. (*See* Specification page 3, lines 1-9.)

One embodiment, which is the subject of Independent Claim 31, is directed to a method for identifying a corresponding session for a packet. (*See, e.g.,* Specification page 3, lines 19-20.) The method includes the steps:

(a) in a first session, a first endpoint transmitting first and second sets of packets, respectively, to a session monitor and a second endpoint (*See, e.g.,* Specification page 2, lines 14-15), wherein the first and second sets of packets have differing information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), wherein each packet in the first set of packets is used for determining network performance information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier (*See, e.g.,* Specification page 2, lines 14-19; page 3, lines 12-18; page 3, line 21 to page 4, line 2; page 5, lines 6-15; page 6, lines 4-6);

(b) the session monitor receiving at least a first packet in the first packet set, the first packet comprising at least the network address and session identifier associated with the first endpoint (*See, e.g.,* Specification page 8, lines 15-21; Fig. 2 (step 200));

(c) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures (*See, e.g.,* Specification page 9, line 3 to page 10, line 2; Fig. 2 (steps 204 and 212)), the first set of data structures comprising active session entries, each entry in the first

set of data structures having at least network addresses for each of the endpoints to the corresponding session (*See, e.g.,* Specification page 7, lines 12-13; page 8, lines 3-11; Fig. 3 (element 308));

(d) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, updating the corresponding entry to include the network performance information associated with the at least a first packet (*See, e.g.,* Specification page 9, line 20 to page 10, line 2; Fig. 2 (step 216));

(e) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures (*See, e.g.,* Specification page 10, lines 3-6; Fig. 2 (step 220)), the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session (*See, e.g.,* Specification page 7, lines 11-12; page 7, line 16, to page 8, line 2; Fig. 3 (element 304)); and

(f) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, updating the entry to include the performance information associated with the at least a first packet (*See, e.g.,* Specification page 10, lines 7-11; Fig. 2 (step 224)).

Another embodiment, which is the subject of Independent Claim 40, is directed to a network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions (*See, e.g.,* Specification page 7, lines 9-10; Fig. 3 (element 300)); and

(ii) first endpoint and second endpoints (*See, e.g.,* Specification page 3, lines 21-22; Fig. 1 (elements A and B)), the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint (*See, e.g.,* Specification page 2, lines 14-15), wherein the first and second sets of packets have differing information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), wherein each packet in the first set of packets is used by the session monitor to determine

network performance information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier (*See, e.g.,* Specification page 2, lines 14-19; page 3, lines 12-18; page 3, line 21 to page 4, line 2; page 5, lines 6-15; page 6, lines 4-6), the session monitor comprising:

(a) an input operable to receive at least a first packet in the first packet set , the first packet comprising at least the network address and session identifier associated with the first endpoint (*See, e.g.,* Specification page 8, lines 15-21; Fig. 2 (step 200); Fig. 3 (element 300)); and

(b) a matcher (*See, e.g.,* Specification page 9, lines 3-4; Fig. 3 (element 316)) operable to:

(b1) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures (*See, e.g.,* Specification page 9, line 3 to page 10, line 2; Fig. 2 (steps 204 and 212)), the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session (*See, e.g.,* Specification page 7, lines 12-13; page 8, lines 3-11; Fig. 3 (element 308));

(b2) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, update the corresponding entry to include the performance information associated with the at least a first packet (*See, e.g.,* Specification page 9, line 20 to page 10, line 2; Fig. 2 (step 216));

(b3) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures (*See, e.g.,* Specification page 10, lines 3-6; Fig. 2 (step 220)), the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session (*See, e.g.,* Specification page 7, lines 11-12; page 7, line 16, to page 8, line 2; Fig. 3 (element 304)); and

(b4) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, update the entry to include the performance information associated with the at least a first packet (*See, e.g.,* Specification page 10, lines 7-11; Fig. 2 (step 224)).

Another embodiment, which is the subject of Independent Claim 48, is directed to a method performed by a network. The network comprises:

(i) a session monitor operable to track network performance for a plurality of sessions (*See, e.g.,* Specification page 7, lines 9-10; Fig. 3 (element 300)); and

(ii) first endpoint and second endpoints (*See, e.g.,* Specification page 3, lines 21-22; Fig. 1 (elements A and B)), the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint (*See, e.g.,* Specification page 2, lines 14-15), wherein the first and second sets of packets have differing information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), wherein each packet in the first set of packets is used by the session monitor to determine network performance information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier (*See, e.g.,* Specification page 2, lines 14-19; page 3, lines 12-18; page 3, line 21 to page 4, line 2; page 5, lines 6-15; page 6, lines 4-6).

The method comprises:

(a) the first endpoint receiving at least a first packet communicated between the first endpoint and a second endpoint to a first session , the first packet comprising an address of the first endpoint on the network, an address of the second endpoint on the network, and voice information, and being associated with the second packet set (*See, e.g.,* Specification page 1, lines 9-21; page 10, line 20, to page 11, line 1; Fig. 4 (step 400)); and

(b) the first endpoint transmitting at least a second packet to a session monitor (*See, e.g.,* Specification page 11, lines 2-12; Fig. 4 (step 400)), the at least a second packet including the respective first and second network addresses of the first and second endpoints and being associated with the first packet set (*See, e.g.,* Specification page 11, lines 7-12; Fig. 4 (step 412)).

Yet another embodiment, which is claimed in Independent Claim 51, is directed to a network. The network comprises:

(i) a session monitor operable to track network performance for a plurality of sessions (*See, e.g.,* Specification page 7, lines 9-10; Fig. 3 (element 300)); and

(ii) first endpoint and second endpoints (*See, e.g.,* Specification page 3, lines 21-22; Fig. 1 (elements A and B)), the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint (*See, e.g.,* Specification page 2, lines 14-15), wherein the first and second sets of packets have differing information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), wherein each packet in the first set of packets is used by the session monitor to determine network performance information (*See, e.g.,* Specification page 1, lines 9-17; page 2, lines 14-15), and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier (*See, e.g.,* Specification page 2, lines 14-19; page 3, lines 12-18; page 3, line 21 to page 4, line 2; page 5, lines 6-15; page 6, lines 4-6).

The first endpoint comprises:

(a) an input operable to receive at least a first packet communicated between the first and second endpoints to a first session, the first packet comprising a network address of the first endpoint, a network address of the second endpoint, and voice information, and being associated with the second packet set (*See, e.g.,* Specification page 1, lines 9-21; page 10, line 20, to page 11, line 1; Fig. 1 (elements A and B); Fig. 4 (step 400)); and

(b) a transmitter operable to transmit at least a second packet to a session monitor (*See, e.g.,* Specification page 11, lines 2-12; Fig. 1 (elements A and B); Fig. 4 (step 400)), the at least a second packet including the respective first and second network addresses of the first and second endpoints and being associated with the first packet set (*See, e.g.,* Specification page 11, lines 7-12; Fig. 4 (step 412)).

Yet another embodiment, which is claimed in Independent Claim 54, is directed to a session packet for transmission on a network. The packet comprises:

a source network address of a first participant to a Voice over Internet Protocol (VoIP) session (*See, e.g.,* Specification page 5, lines 6-15; page 10, line 21, to page 11, line 1; page 11, lines 7-11);

a destination network address associated with a session monitor (*See, e.g.,* Specification page 11, lines 7-11);

a network address of a second participant to the VoIP session (*See, e.g.,* Specification page 5, lines 6-15; page 10, line 21, to page 11, line 1; page 11, lines 7-11); and

session information associated with the VoIP session (*See, e.g.,* Specification page 5, lines 6-15; page 10, line 21, to page 11, line 1; page 11, lines 7-11).

(VI) GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Whether Claims 31, 33, 35, 38-39, 42, 44, 47, 50, and 53 are unpatentable under 35 U.S.C.§103(a) over U.S. Patent No. 6,529,475 [hereinafter "Wan"] in view of U.S. Patent Application Publication No. 2002/0105911 [hereinafter "Pruthi"] and further in view of U.S. Patent No. 6,463,474 [hereinafter "Fuh"].

Whether Claims 32 and 41 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

Whether Claims 34-37 and 43-46 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

Whether Claims 48, 51, and 54-56 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

Whether Claims 49 and 52 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

(VII) ARGUMENT

1. Rejection of Claims 31, 33, 35, 38-39, 42, 44, 47, 50, and 53 under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

The Office argues that Wan teaches the invention substantially as claimed but cites Pruthi for the teaching of determining whether the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures and, if so, updating the corresponding entry to include the associated network performance information and Fuh for the teaching of updating a new entry in a second set of data structures when the network address is not included in the first set of data structures.

In order for a rejection under 35 U.S.C.§103(a) to be proper, there must be some suggestion or motivation to modify the reference or to combine the reference teachings, coupled with a reasonable expectation of success, and the prior art reference or references must teach or suggest all of the claim limitations. In re Vaeck, 947 F.2d 488 (Fed. Cir. 1991).

Appellants respectfully disagree with the Examiner's position that Claims 31, 33, 35, 38-39, 42, 44, 47, 50, and 53 are obvious in view of the combination of Wan, Pruthi, and Fuh.

Although Wan discloses periodic transmission of control packets to all participants in a session (col. 6, lines 5-7), it does not disclose periodic transmission of control packets to one or more session endpoints and a session monitor (see col. 5, lines 49-54 and col. 6, lines 5-7), and is silent regarding tracking active RTCP sessions to pair packetized network performance information with the session. Wan is directed to reducing congestion of real time data traffic on a multimedia communications network having a traffic control mechanism. Wan first extracts, from data traffic, information regarding congestion of the network. A call admission control module in a central server regulates congestion by receiving, from the congestion monitors, traffic information, using the information to analyze congestion status, and communicating instructions to the network to reduce congestion.

The Examiner responds by stating that "in Wan's network monitoring system, a plurality of RTCP monitors scan through RTCP packets exchanging between 'computers 104/ and 108' those share functionality with 'first and second endpoint' as claimed" (Advisory Action at page 2, paragraph 1) and that "Wan discloses 'network RTCP monitors (110)' which is interpreted as network destination" (*id.* at para. 8). The Examiner ignores the clear language of Wan. Wan extracts, from data traffic, congestion information using a network of congestion monitors (which are different from RTCP session monitors) "tapping into" RTCP packet flows (col. 6, lines 34-36). "Tapping into" refers to packet sniffing by the congestion monitor and ***not*** to the congestion monitor being a control packet addressee or destination of packet transmission. Wan, in fact, describes congestion monitors as "stand-alone boxes that can tap into a router or switch to monitor RTCP flows" (col. 6, lines 33-35) and as packet scanners (col. 4, lines 61-63, and col. 6, lines 36-41). Fig. 2 of Wan shows the monitors 110 acting, not as network nodes for receiving packets, but as packet sniffers. Simply put, the Examiner has mischaracterized congestion monitors with RCTP monitors; they are not the same.

Pruthi also teaches packet sniffing and teaches away from a session monitor being a packet addressee. In Pruthi, et al., a network monitor 102 extracts or sniffs packets from the bit stream on communication line 104 and converts them to records stored in memory (paras. [0035] and [0067]). The records are generated by first determining the type (protocol or layer) of each packet (step 414) and then filtering the packets (step 416) based on their determined types. An index is generated (step 418) for each packet, and the packet is then converted into an indexed record (step 420). The time when the network monitor received each IP packet is used as an index for each IP packet. Exemplary information retained respecting each packet includes the type of the packet, the size of the packet, a packet number, source or destination address, an interface number, an application, and an associated session identifier. Using the index, statistics measured include packet size distributions, protocol distributions, bandwidth usage per client, bandwidth usage by domain, average response time per server, average round-trip time between server-client pair, and performance metrics.

Regarding invasive monitoring techniques, such as transmitting control packets to a session monitor, Pruthi states in paragraph [0008]:

> [0008] Network monitors of the current art generally *intrude* into the network in order to evaluate or estimate network performance. The reference "TCP/IP Ilustrated, Volume I--The Protocols," Chapters 7 and 8, available from Addison-Wesley Publishing Co., 1994, describes one such technique. To estimate round-trip times for "packets" of information in the internet, the network monitor injects additional packets into the network and follows the travel of such additional packets. *Thus, the very process of determining network performance itself further degrades performance by adding additional packets of information to the traffic.*:

(Emphasis supplied.) Accordingly, Pruthi teaches that transmission of control packets to both the session participants and session monitor is undesirable as it would further degrade network performance.

Pruthi further fails to address the use of differing sets of data structures to include entries for fully and partially identified active sessions. In the Advisory Action, the Examiner states:

> In Pruthi's network monitoring system, a network monitor monitors communication sessions between network computers; each entry of the Pruthi's communication sessions record includes a plurality of element such as record index, source address, destination address . . . etc. the recorder generator read the previously stored indexed record to determine if existing common previous stored indexed record, then it combines a new record updated network performance information into the previous stored indexed record. The Pruthi's network monitor may recursively collect and analyze network performance data based on previously generated stored packets: ([0046]-[0048]; [0065]-[0066]; [0040]).

The Examiner's position is flawed. Not only is Pruthi silent on matching up orphaned session packets with the appropriate session identification data structures but also in Pruthi there is no need for such matching. In Pruthi, each packet, when extracted from the packet flows, already includes source and destination addresses and the appropriate (unique) session identifier. Pruthi is sniffing packets exchanged directly between two endpoints that, for a given session, will always include the same two IP endpoint addresses either as source or destination (depending upon the direction of packet flow) as the packets are transmitted between endpoints and are not sent to the monitor. Thus, the two IP addresses will appear in

the original index and in any subsequently generated index. In other words, there will be no set of data structures in which one of the IP addresses is unknown. In contrast, in the claimed architecture, differing endpoints (the packet sources) are *separately* sending control packets related to the same session *to the same session monitor* (the packet destination). The control packets in the claimed architecture therefore do not include both endpoint addresses. Matching is therefore needed to identify, for a given session, all of the session participant's addresses and respective session identifiers, particularly where endpoint session identifiers are duplicated. This is an ongoing problem in packet-based live voice communications because, under protocols such as RTP, each session participant is given a separate session identifier. Thus, until the packet streams are matched, the session monitor knows, for each discrete packet stream or each session identifier, only the IP address of the corresponding endpoint.

Fuh is directed to authentication and access control and teaches nothing regarding architectures for transmitting control packets to session participants and a session monitor let alone the use of differing sets of data structures to include entries for fully and partially identified active sessions. In Fuh, et al., a network device is configured to intercept network traffic initiated from a client and directed toward a network resource and to locally authenticate the client. Authentication is carried out by comparing source IP address in the header against an Access Control List and, if successful, searching authentication caches for the source IP address. When a corresponding cache is located, the client is authenticated. When a corresponding cache is not located, a linked authentication cache is created. If the source IP address does not match any of the ACL entries, the packet is denied passage.

None of the cited references teach or suggest the possible existence of packets from different sessions having a common session identifier and therefore fail to provide any incentive or motivation to use differing packet structures to match up packets with appropriate sessions. Wan fails to even mention session identifiers, let alone the possibility that each session endpoint has a corresponding session identifier. In both Wan and Pruthi, the session endpoints involved in each session being analyzed are already known. In Pruthi,

the session identifier is, unlike the claimed architecture, associated with the session and not the endpoints and, unlike the claimed architecture, unique. In the Pruthi architecture, each session, and its endpoints, are associated with only one session identifier and not multiple session identifiers. There is therefore no possibility for mismatching packets with incorrect sessions and therefore no need to modify the prior art architectures to realize the claimed invention.

Finally, the Examiner argues that (a) using first and second data structure sets to identify unidentified and identified sessions, respectively, and (b) transmitting separate packets to the other endpoint and a performance monitor are not in the rejected claims. (Advisory Action at page 2, para. 11.) Applicant disagrees. Feature (a) is claimed in independent claims 31 (see steps (c) and (e)) and 40 (see operations (b1) and (b3)) and dependent claims 36, 37, 45, 46, 50, and 53, and feature (b) is claimed in independent claims 31 (step (a)), 40 (element (ii)), 48 (element (ii)), and 51 (element (ii)). Applicant notes "unidentified" means simply that the other endpoint(s) to a packet stream has not yet been identified fully while "identified" means that the other endpoint(s) to the packet stream has been identified fully.

2. Rejection of Claims 32 and 41 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

Dependent claims 32 and 41 require at least some of the packets in the second set of packets to include media information associated with the first session, and, in steps (c) and (e), a corresponding entry to be identified using the network address and session identifier of the first endpoint.

The cited references do not teach or suggest matching endpoint addresses and session identifiers in different packets with one another to determine the various session participants.

Wan teaches, at col. 8, lines 42-48, collecting and periodically forwarding to a central server "statistical information" from RTCP packets regarding the congestion status of the network. Wan says nothing about whether session endpoint addresses and/or session identifiers are part of the collected "statistical information." Wan says nothing about using

both network address and session identifier of an endpoint to match packets with a corresponding entry. This is necessitated by the lack of knowledge of all participant endpoint addresses and endpoint session identifiers for certain sessions. Pruthi teaches the use of a unique ATM session identifier alone (only one of which is assigned to each session) to pair up packets with appropriate records. (*See* example at ¶¶ 0047 and 0048.)

3. Rejection of Claims 34-37 and 43-46 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

Dependent claims 34 and 43 require the session monitor to:

determine whether a pair of session entries in the second set of data structures pertain to a common session; and

when the second set of data structures includes a pair of session entries pertaining to a common session, remove the pair of entries from the second set of data structures and add the pair of session entries to a common session entry in the first set of data structures. Dependent claims 35 and 44 further require, when the at least one of the first endpoint's network address and session identifier are not in the first and second sets of data structures, the at least one of the first endpoint's network address and session identifier are added to the second set of data structures.

As noted, both Wan and Pruthi fail to teach the use of first and second sets of data structures to contain network performance information respecting unidentified and identified sessions, respectively, let alone adding such information to the second set of data structures as initial session packets are received. (*See also* dependent claims 36-37, 45-46, 50, and 53.)

4. Rejection of Claims 48, 51, and 54-56 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

None of the references teach an endpoint sending to the session monitor a packet including not only the source endpoint's network address but also the network address(es) of the other session participant endpoint(s). As noted, in VoIP control signaling, such as RTCP, each participant sends, to the session monitor, control packets containing the source

participant's address and session identifier and network performance information. The rejected claims are directed to a novel architecture in which each participant extracts the other participants' addresses from the voice payload, or second set of, packets and includes not only the sending participant's and session monitor's addresses and sending participant's session identifier but also the address(es) and session identifier(s) of the other participant(s). Dependent Claim 55 specifically requires the same session packet to include not only multiple endpoint addresses but also multiple session identifiers corresponding to the participants.

The Examiner's reasoning in rejecting these claims is that "Pruthi discloses the session monitor used for monitoring data packets sent/and received from/and to first computers C1 and second computer C2 and that it would have been obvious in the art to know that data packets should include the respective network addresses of the first computer C1/and the second computer C2" (Advisory Action at para. 6) and that "Wan's network RTCP monitors can support for controlling VoIP communications between communication participants" (*id.* at para. 9). ***The Examiner's argument completely ignores the fact that none of the cited references teach or suggest sending any packets directly to a session monitor let alone sending packets including addresses and session identifiers of session participants.*** Wan and Pruthi are directed to packet sniffers, which remove selected packets from packet flows. The extracted packets are not transmitted (or addressed) to the session monitor and therefore include no address associated with the session monitor. ***The Examiner's argument further ignores the fact that, even if Wan and Pruthi taught each participant sending packets to a session monitor, the packet would include only the source participant and session monitor addresses and not the address(es) and session identifier(s) of the other session participants.***

5. Rejection of Claims 49 and 52 are unpatentable under 35 U.S.C.§103(a) over Wan in view of Pruthi and further in view of Fuh.

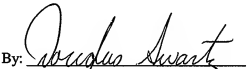
Dependent claims 49 and 52 require the first endpoint to transmit at least a second packet to a session monitor, when a value of a flag has a first predetermined value. The second packet includes the addresses of the session participants and session monitor and session identifier. The flag indicates whether or not the sending, or second, endpoint already sent a packet to the session monitor. The flag thus creates

a bimodal method of operation in which, depending on the flag value, a further packet may or may not be sent to the session monitor.

As noted, neither Wan nor Pruthi teach or suggest transmitting, to a session monitor, a packet containing multiple session endpoint addresses and session information. Pruthi teaches away from this step by teaching that extracting packets being exchanged between session endpoints avoids intruding into the network and adversely impacting network performance.

For at least the reasons elaborated upon in this brief, Appellants submit that the rejection of the pending claims in view of the combination of Wan, Pruthi, and Fuh should be withdrawn.

Respectfully submitted,
SHERIDAN ROSS P.C.

By: 
Douglas W. Swartz
Registration No. 37,739
1560 Broadway, Suite 1200
Denver, Colorado 80202-5141
(303) 863-9700

Date: Nov. 7, 2007

(VIII) CLAIMS APPENDIX

1-30. (Canceled)

31. A method for identifying a corresponding session for a packet, comprising:

(a) in a first session, a first endpoint transmitting first and second sets of packets, respectively, to a session monitor and a second endpoint, wherein the first and second sets of packets have differing information, wherein each packet in the first set of packets is used for determining network performance information, and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier;

(b) the session monitor receiving at least a first packet in the first packet set, the first packet comprising at least the network address and session identifier associated with the first endpoint;

(c) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(d) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, updating the corresponding entry to include the network performance information associated with the at least a first packet;

(e) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session; and

(f) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, updating the entry to include the performance information associated with the at least a first packet.

32. The method of claim 31, wherein at least some of the packets in the second set of packets comprise media information associated with the first session, and wherein, in steps (c) and (e), a corresponding entry is identified using the network address and session identifier of the first endpoint.

33. The method of claim 31, wherein step (e) is performed when the at least one of the first endpoint's network address and session identifier fail to correspond to an entry in the first set of data structures, wherein the electronic network address is at least one of a port and transport address, and further comprising before the determining step (c):

(b1) parsing the at least a first packet for at least one selected field; and

(b2) determining whether the network address of the second endpoint is in the selected field, wherein, when the network address of the second endpoint is in the selected field, steps (e)-(f) are not performed and, when the network address of the second endpoint is not in the selected field, steps (e)-(f) are performed.

34. The method of claim 31, wherein the network performance information comprises statistics about the media packets in the second set of packets and further comprising:

(g) determining whether a pair of session entries in the second set of data structures pertain to a common session; and

(h) when the second set of data structures includes a pair of session entries pertaining to a common session, removing the pair of entries from the second set of data structures and adding the pair of session entries to a common session entry in the first set of data structures.

35. The method of claim 31, wherein, when the at least one of the first endpoint's network address and session identifier are not in the first and second sets of data structures, the at least one of the first endpoint's network address and session identifier is added to the second set of data structures.

36. The method of claim 31, wherein the packets in the first set of packets are defined by the Real Time Transfer Control Protocol, wherein the packets in the second set of packets are defined by one of the Real Time Transfer Control Protocol and the Real Time Protocol, wherein the performance information comprise statistics respecting at least one of jitter, packet loss, and round-trip time, wherein step (b) comprises the substeps:

(b1) parsing the at least a first packet to locate selected fields comprising the transport address of the sending endpoint, the session identifier of the sending endpoint, the transport address of the destination endpoint, and the session identifier of the destination endpoint, wherein the first endpoint is the source endpoint and the second endpoint is the destination;

(b2) when the at least a first packet comprises the network address of the second endpoint, updating a set of data structures to include the second endpoint's network address; and

(b3) when the at least a first packet does not comprise the network address of the second endpoint, updating a corresponding entry in one of the first and second sets of data structures.

37. The method of claim 32, wherein the first set of data structures comprises, for each active session, a transport address of each of the endpoints participating in the session, the session identifiers for each of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, wherein the second set of data structures comprises, for each active session, a transport address of at least one of the endpoints participating in the session, a session identifier for at least one but less than all of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, and wherein the performance information comprises at least one of jitter, packet loss, and packet round-trip time, wherein the media information comprises voice data, and wherein the packets in the first set of packets do not contain media information.

38. The method of claim 31, wherein steps (d) and (e) are not performed when the at least a first packet includes the network address of the second endpoint and wherein the session monitor performs steps (c) and (e).

39. A computer readable medium comprising processor executable instructions to perform the steps of claim 31.

40. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing

information, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier, the session monitor comprising:

(a) an input operable to receive at least a first packet in the first packet set, the first packet comprising at least the network address and session identifier associated with the first endpoint; and

(b) a matcher operable to:

(b1) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(b2) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, update the corresponding entry to include the performance information associated with the at least a first packet;

(b3) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session; and

(b4) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, update the entry to include the performance information associated with the at least a first packet.

41. The session monitor of claim 40,wherein at least some of the packets in the second set of packets comprise media information associated with the first session, and wherein, in operations (b1) and (b3), a corresponding entry is identified using the network address and session identifier of the first endpoint.

42. The session monitor of claim 40, wherein operation (b3) is performed when the at least one of the first endpoint's network address and session identifier fail to correspond to an entry in the first set of data structures, wherein the electronic network address is at least one of a port and transport address, and further comprising:

(c) a parser operable to parse the at least a first packet for at least one selected field and determine whether the network address of the second endpoint is in the selected field, wherein, when the network address of the second endpoint is in the selected field, operations (b1)-(b4) are not performed and, when the network address of the second endpoint is not in the selected field, operations (b1)-(b4) are performed.

43. The session monitor of claim 40, wherein the network performance information comprises statistics about the media packets in the second set of packets and wherein the session monitor is further operable to:

(b5) determine whether a pair of session entries in the second set of data structures pertain to a common session; and

(b6) when the second set of data structures includes a pair of session entries pertaining to a common session, remove the pair of entries from the second set of data structures and adding the pair of session entries to a common session entry in the first set of data structures.

44. The session monitor of claim 40, wherein, when the at least one of the first endpoint's network address and session identifier are not in the first and second sets of data structures, the at least one of the first endpoint's network address and session identifier is added to the second set of data structures.

45. The session monitor of claim 40, wherein the packets in the first set of packets are defined by the Real Time Transfer Control Protocol, wherein the packets in the second set of packets are defined by one of the Real Time Transfer Control Protocol and the Real Time Protocol, wherein the performance information comprise statistics respecting at least one of jitter, packet loss, and round-trip time, and further comprising:

(c) a parser operable to parse the at least a first packet to locate selected fields comprising the transport address of the sending endpoint, the session identifier of the sending endpoint, the transport address of the destination endpoint, and the session identifier of the destination endpoint, wherein the first endpoint is the source endpoint and the second endpoint is the destination and wherein the session monitor is further operable to:

(b5) when the at least a first packet comprises the network address of the second endpoint, update a set of data structures to include the second endpoint's network address; and

(b6) when the at least a first packet does not comprise the network address of the second endpoint, update a corresponding entry in one of the first and second sets of data structures.

46. The session monitor of claim 41, wherein the first set of data structures comprises, for each active session, a transport address of each of the endpoints participating in the session, the session identifiers for each of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, wherein the second set of data structures comprises, for each active session, a transport address of at least one of the endpoints participating in the session, a session identifier for at least one but less than all of the endpoints participating in the session, and performance information corresponding to packets exchanged in the session, and wherein the performance information comprises at least one of jitter, packet loss, and packet round-trip time, wherein the media information comprises voice data, and wherein the packets in the first set of packets do not contain media information.

47. The session monitor of claim 40, wherein operations (b3) and (b4) are not performed when the at least a first packet includes the network address of the second endpoint.

48. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing information, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier, a method comprising:

(a) the first endpoint receiving at least a first packet communicated between the first endpoint and a second endpoint to a first session, the first packet comprising an address of the first endpoint on the network, an address of the second endpoint on the network, and voice information, and being associated with the second packet set; and

(b) the first endpoint transmitting at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being associated with the first packet set.

49. The method of claim 48, wherein step (a) comprises the substep:

(a1) determining a value of a flag in the at least a first packet;

and wherein, when the flag has a first predetermined value, performing step (b) and, when the flag has a second predetermined value, not performing step (b).

50. The method of claim 48, further comprising:

(c) the session monitor receiving at least a second packet in the first packet set, the second packet comprising at least the network address and session identifier associated with the first endpoint;

(d) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(e) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, updating the corresponding entry to include the network performance information associated with the at least a second packet;

(f) determining whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session; and

(g) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, updating the entry to include the performance information associated with the at least a second packet.

51. In a network, the network comprising:

(i) a session monitor operable to track network performance for a plurality of sessions; and

(ii) first endpoint and second endpoints, the first endpoint being operable to transmit first and second sets of packets, respectively, to the session monitor and the second endpoint, wherein the first and second sets of packets have differing information, wherein each packet in the first set of packets is used by the session monitor to determine network performance information, and wherein each of the first and second endpoints has an associated electronic address on a network and a session identifier, the first endpoint comprising:

(a) an input operable to receive at least a first packet communicated between the first and second endpoints to a first session, the first packet comprising a network address of the first endpoint, a network address of the second endpoint, and voice information, and being associated with the second packet set; and

(b) a transmitter operable to transmit at least a second packet to a session monitor, the at least a second packet including the respective first and second network addresses of the first and second endpoints and being associated with the first packet set.

52. The network of claim 51, wherein the first packet includes a flag and wherein, when the flag has a first predetermined value, the transmitter transmits the at least a second packet and, when the flag has a second predetermined value, the transmitter does not transmit the at least a second packet.

53. The network of claim 51, wherein the session monitor comprises:

(a) an input operable to receive at least a second packet in the first packet set, the second packet comprising at least the network address and session identifier associated with the first endpoint; and

(b) a matcher operable to:

(b1) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a first set of data structures, the first set of data structures comprising active session entries, each entry in the first set of data structures having at least network addresses for each of the endpoints to the corresponding session;

(b2) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the first set of data structures, update the corresponding entry to include the performance information associated with the at least a second packet;

(b3) determine whether at least one of the first endpoint's network address and session identifier correspond to an active session entry recorded in a second set of data structures, the second set of data structures having active session entries, each of the entries in the second set of data structures failing to comprise network addresses for each of the endpoints to the corresponding session; and

(b4) when at least one of the first endpoint's network address and session identifier correspond to an active session entry in the second set of data structures, update the entry to include the performance information associated with the at least a second packet.

54. A session packet for transmission on a network, comprising:

a source network address of a first participant to a Voice over Internet Protocol (VoIP) session;

a destination network address associated with a session monitor;

a network address of a second participant to the VoIP session; and

session information associated with the VoIP session.

55. The session packet of claim 54, further comprising:

a first session identifier associated with the first participant; and

a second session identifier associated with the second participant.

56. The session packet of claim 54, wherein the contents of the session packet are defined by the Real Time Control Protocol.

(IX) EVIDENCE APPENDIX

Primarily for the convenience of the reader, copies of the documents relied upon by the Examiner as to grounds of rejection to be reviewed on appeal are provided here. These documents include:

Wan Patent (U.S. Patent No. 6,529,475)

Pruthi Patent Application (U.S. Patent App. No. 2002/0105911)

Fuh Patent (U.S. Patent No. 6,463,474).

(X) RELATED PROCEEDINGS APPENDIX

None.